Research study on the introduction of CDS into ZTA's 5 Pillars*

Yeomin Lee and Jungsoo Park†
Kangnam University , Gi Heung, South Korea.
{1252037, jspark} @kangnam.ac.kr

Abstract

This research presents a framework for applying Cross-Domain Solutions (CDS) to the five pillars of Zero Trust Architecture (ZTA), demonstrating that this integration is critical for strengthening the overall model.

Keyword: Zero Trust Architecture, CDS, ZTA 5 Pillars, Strengthening ZTA with CDS

1 Introduction

Based on the principle of "Never Trust, Always Verify," Zero Trust Architecture (ZTA) protects systems by continuously authenticating all access and applying consistent security policies across its five core pillars: Identity, Device, Network, Application, and Data.

2 Background

A. The Concept and 5 Pillars of Zero Trust

Zero Trust Architecture (ZTA) is a security model founded on the principle of "Never Trust, Always Verify" which continuously authenticates all internal and external access. Based on its five core pillars— Identity, Device, Network, Application, and Data—ZTA protects the system by applying consistent security policies across each domain.

B. CDS

It is a specialized security solution that securely controls and filters data flow between network environments with different security levels, according to policy.

3 Analysis

A. Identity Pillar

Thomas et al. [1] standard connects to MLS (Multi-Level Security) CDS. This combination securely manages and synchronizes identity information across domains with different security levels.

B. Device Pillar

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-41, December 16-18, 2025, Sapporo, Japan.
† Corresponding author

To address poor device trust and the inefficiency of using separate devices for each network, Everfox [2] proposes an Access-type CDS. A solution like a Trusted Thin Client (TTC) ensures device integrity from boot-up and provides a single, trusted endpoint for securely accessing multiple networks at once.

C. Network Pillar

Alam et al. [3] link O-RAN architecture and network slicing with a Transfer CDS. This solves the problem of redundant security tasks caused by network isolation by enabling trusted software functions, thereby ensuring complete protection for sensitive information.

D. Applications Pillar

Everfox [2] also explains how Transfer CDS solves problems for the Applications pillar. The primary issue was the lack of a secure method for applications on networks with different security levels to exchange data via API. A Transfer CDS integrates with API gateways, offering the expected benefit of enabling secure API calls and data transfers between these different networks.

E. Data Pillar

DoD [4] emphasizes protecting the data itself as a key feature of the Data Pillar, utilizing technologies such as Data Tagging, encryption, DRM, DLP. This concept of enforcing data-centric security policies on the actual data flow aligns precisely with the core function of a Transfer CDS, which is to read the data's security labels and inspect its content to execute policies.

4 Result

Cross-Domain Solutions (CDS) are crucial for strengthening the pillars of Zero Trust Architecture (ZTA) because network isolation remains necessary for high-security systems, even in a data-centric model. Therefore, policy, analytics, and data security require an integrated, cyberspace-wide implementation.

Acknowledgment

This work was supported by "Contract-Based Graduate Enrollment Quotas Program" of Korea Industrial Technology Association (KOITA) funded by Ministry of Science and ICT(MSIT).

References

[1] Baumer, T., Müller, M., & Pernul, G. (2023). System for Cross-Domain Identity Management (SCIM): Survey and Enhancement With RBAC. *IEEE*

[2] Multilevel Zero Trust Whitepaper: Enabling Zero Trust with Cross Domain Solutions. Everfox.

[3] Alam, K., Habibi, M. A., Tammen, M., Krummacker, D., Saad, W., Di Renzo, M., Melodia, T., Costa-Pérez, X., Debbah, M., Dutta, A., & Schotten, H. D. (2025). A Comprehensive Tutorial and Survey of O-RAN: Exploring Slicing-aware Architecture, Deployment Options, Use Cases, and Challenges. IEEE

[4] Defense Information Systems Agency & National Security Agency. (2022, July). Department of Defense (DoD) Zero Trust Reference Architecture (Version 2.0).